Master the 250-604 Exam: Study Guide Plus Practice Questions

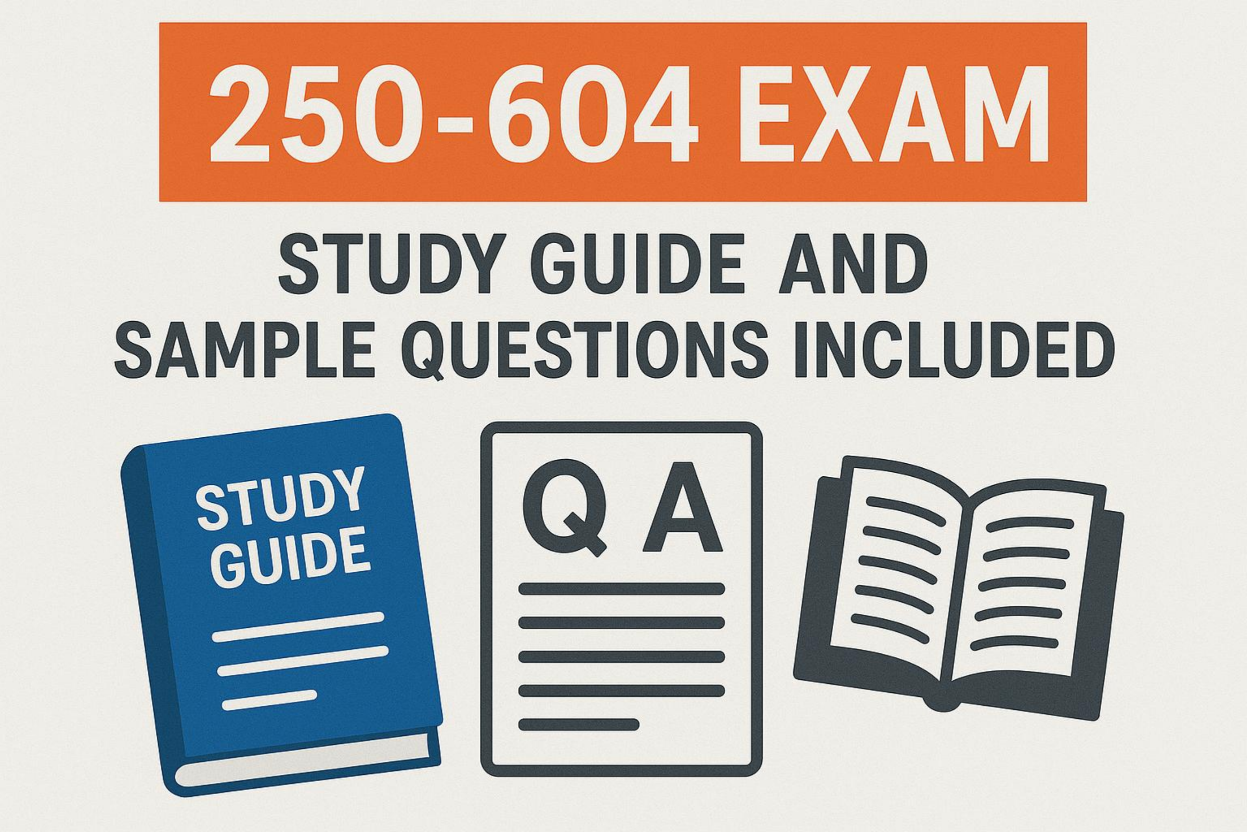
Broadcom Certification

Find everything you need to pass the Broadcom 250-604 exam on your first attempt right here: https://bit.ly/4lI8FUW. Access a complete set of resources—including the syllabus, study guide, practice tests, recommended books, and more—all in one place. With the right preparation, mastering the exam domains becomes easier, and earning the Broadcom Symantec Endpoint Security Complete Admin R3 Technical Specialist certification is well within reach.

Certfun.com

How to Earn the 250-604 Broadcom Symantec Endpoint Security Complete Admin R3 Technical Specialist Certification on Your First Attempt?

Earning the Broadcom 250-604 certification is a dream for many candidates. But, the preparation journey feels difficult to many of them. Here we have gathered all the necessary details like the syllabus and essential 250-604 sample questions to get to the Broadcom Symantec Endpoint Security Complete Admin R3 Technical Specialist certification on the first attempt.



250-604 Endpoint Security Complete Admin Technical Specialist Summary:

Exam Name	Broadcom Symantec Endpoint Security Complete Admin R3 Technical Specialist
Exam Code	250-604
Exam Price	$250 (USD)
Duration	90 mins
Number of Questions	75
Passing Score	70%
Books / Training	Symantec Endpoint Security Complete Administration Symantec Endpoint Security Complete – Basic Administration
Schedule Exam	Broadcom
Sample Questions	Broadcom Endpoint Security Complete Admin Technical Specialist Sample Questions
Practice Exam	**Broadcom 250-604 Certification Practice Exam**

Let's Explore the Broadcom 250-604 Exam Syllabus in Detail:

Topic	**Details**
Introduction to Symantec Endpoint Security Complete	- Understand SES Complete Architecture. - Describe the benefits of SES Complete Cloud-based management. - Describe the various methods for enrolling SES endpoint agents.
Configuring SES Complete Security Controls	- Understand how policies are used to protect endpoint devices. - Understand the Threat landscape and the MITRE ATT&CK Framework. - Describe how SES Complete can be used in preventing an attacker from accessing the environment. - Describe how SES Complete prevents threat execution. - Describe how SES Complete prevents threat persistence. - Describe how SES Complete prevents privilege escalation. - Describe how SES Complete prevents defense evasion. - Describe how SES Complete prevents device discovery. - Describe how SES Complete blocks Command & Control communication. - Describe how SES Complete works to block data exfiltration. - Describe SES Complete content update types and how they are distributed to endpoints. - Describe SES Complete policy versioning and its use.
Responding to Threats with ICDm	- Describe the ICDm security control dashboards and their use. - Understand how ICDm is used to identify threats in the environment.

Topic	Details
	- Describe the incident lifecycle and steps required to identify a threat. - Describe the ways in which ICDm can be used to remediate threats. - Describe how to use ICDm to configure administrative reports.
Endpoint Detection and Response	- Describe the requirements to enable Endpoint Detection and Response in the ICDm management console. - Describe how EDR assists in identifying suspicious and malicious activity. - Describe how EDR aids in investigating potential threats. - Describe the configuration and use of the Endpoint Activity Recorder. - Understand the use of LiveShell for incident response. - Describe how to use EDR to retrieve and submit files for analysis. - Describe how EDR can be used to quarantine endpoint devices. - Describe how EDR can be used to block and quarantine suspicious files.
Attack Surface Reduction	- Describe Behavior Prevalence the use of the SES Complete Behavioral Insights and Policy Tuning Widget. - Describe how the SES Complete Heatmap can be used to prevent unwanted application behaviors. - Describe SES Complete policy adaptations and behavioral tuning. - Describe the SES Complete policy and device groups and how they are used. - Describe the requirements to enable App Control in the ICDm management console. - Describe the process of monitoring drift to further tune App Control policies.
Mobile and Modern Device Security	- Describe the requirements to enable Network Integrity in the ICDm management console. - Describe Network Integrity Policy Configuration and its use. - Describe how Network Integrity works to remediate threats. - Describe how SES Complete's mobile technologies protection against malicious apps. - Describe how SES Complete's mobile technologies protection against malicious networks.
Threat Defense for Active Directory	- Describe the requirements for Threat Defense for Active Directory Installation and Configuration. - Describe the Threat Defense Active Directory policy and its use. - Describe how Threat Defense for Active Directory is used to identify threats.

Topic	Details
	- Describe how Threat Defense for Active Directory protects against misconfigurations and vulnerabilities in an environment.
Working with a Hybrid Environment	- Describe the process for policy migration from SEPM to the ICDm console. - Describe policy precedence in a hybrid configuration. - Understand how Sites and Replication are impacted in a Hybrid environment. - Describe the requirements and process for SEPM integration with the ICDm platform used in a SES Complete Hybrid architecture.

Experience the Actual Exam Structure with Broadcom 250-604 Sample Questions:

Before jumping into the actual exam, it is crucial to get familiar with the exam structure. For this purpose, we have designed real exam-like sample questions. Solving these questions is highly beneficial to getting an idea about the exam structure and question patterns. For more understanding of your preparation level, go through the 250-604 practice test questions. Find out the beneficial sample questions below -

Answers for Broadcom 250-604 Sample Questions

01. Which SES Policy protects against port scan detections?

a) IPS
b) Firewall
c) Device Control
d) Exploit Mitigation

Answer: b

02. What is the name of the cloud-based Management Console that is used to configure and manage an SES Complete implementation?

a) The Integrated Cyber Defense Manager (ICDm)
b) Symantec Endpoint Security Manager (SESM)
c) The Symantec Console (SC)
d) The Integrated Security Protection Manager (ISPm)

Answer: a

03. When should administrators configure automatic quarantine rules for endpoints in ICDm?

a) When endpoints are connected via VPN only
b) When endpoints are consistently offline
c) When a high-severity threat is detected based on predefined behavioral triggers
d) When bandwidth utilization crosses a set threshold

Answer: c

04. Which policy should an administrator edit to utilize the Symantec LiveUpdate server for pre-release content?

a) The System Policy
b) The LiveUpdate Policy
c) The System Schedule Policy
d) The Firewall Policy

Answer: a

05. How does EDR aid in investigating the lateral movement of threats across endpoints in a network?

a) By showing real-time firewall activity logs
b) By integrating third-party authentication alerts
c) By visualizing process-level telemetry across affected endpoints
d) By logging DNS resolution times

Answer: c

06. What is the purpose of Adaptive Protection's Monitor mode?

a) To create a list of risky application behaviors
b) To view the results of Symantec's behavioral global intelligence data analytics
c) To deny unusual application behavior
d) To gain visibility into the operational impact of unusual behavior

Answer: d

07. Why is it important to configure real-time threat identification in ICDm?

a) To accelerate OS patch deployment
b) To reduce licensing costs
c) To enable proactive detection and response
d) To improve email deliverability

Answer: c

08. Which features contribute to blocking data exfiltration in SES Complete? (Choose two)

a) Network Integrity
b) Content Update Optimization
c) Data Loss Prevention Rules
d) Script Runner

Answer: a, c

09. What component of SES Complete handles blocking of suspicious file execution?

a) Activity Recorder
b) Application Control Engine
c) Detection and Prevention Engine
d) Device Integrity Monitor

Answer: c

10. Which antimalware engine detects a malicious file created with a custom packet?

a) Emulator
b) Sapient
c) Core3
d) SONAR

Answer: a